Financial Management Service
Privacy Impact Assessment Template
Name of Project: Enterprise Infrastructure Plan (Enterprise Security Access Administration System (ESAAS))
Project's Unique ID: Enterprise Infrastructure Plan

A. SYSTEM APPLICATION/GENERAL INFORMATION:
1) Does this system contain any information about individuals? Yes.
a. Is this information identifiable to the individual'[1]?

(If there is NO information collected, maintained, or used that is identifiable to the individual in the system, the remainder of the Privacy Impact Assessment does not have to be completed).
Yes.

b. Is the information about individual members of the public? (If YES, a PIA must be submitted with the 0MB Exhibit 300, and with the IT Security C&A documentation).
No.

c. Is the information about employees? (If yes and there is no information about members of the public, the PIA is required for the FMS IT Security C&A process, but is not required to be submitted with the 0MB Exhibit 300 documentation).

Yes.

2) What is the purpose of the system/application?

The purpose of the Enterprise Security Access Administration System is to control via a document processing system, requests for Access to FMS Platform Systems. This system tracks the requests through the approval process.

3) What legal authority authorizes the purchase or development of this system/application?

---

[1] "Identifiable Form" - According to the 0MB Memo M-03-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends
identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

The system was developed in the late 1990's and there is no legal authority to develop.

B. DATA in the SYSTEM:
1) What categories of individuals are covered in the system?

Government employees, contractors, and FRB personnel who require access to FMS Platform systems.

2) What are the sources of the information in the system? Individuals

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?
From the individual who makes an application for access to FMS systems.

b. What Federal agencies are providing data for use in the system? All.

c. What State and local agencies are providing data for use in the system?
All.

d. From what other third party sources will data be collected? N/A.

e. What information will be collected from the employee and the public?
Nothing is coming from the public. Employee, contractor, and FRB Employees are including work phone numbers, addresses, and email addresses. Prior to legal decisions, Social Security Number Information was required, now it is optional.

3) Accuracy, Timeliness, and Reliability
a. How will data collected from sources other than FMS records be verified for accuracy?
They are not.

b. How will data be checked for completeness? None.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models). None.

d. Are the data elements described in detail and documented? If yes, what is the name of the document? No.

C. ATTRIBUTES OF THE DATA:
1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed? Yes.
2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed? No.

3) Will the new data be placed in the individual's record? No.

4) Can the system make determinations about employees/public that would not be possible without the new data? No.

5) How will the new data be verified for relevance and accuracy?

When information is mailed to the requestor, if the mail is returned, we then know that the data is not correct. At that time, we go back to the ISSO of the application, asking them to get the correct information.

6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

Access is only allowed via Key Lists that is controlled by Data Access Control Division (DACD). Information can only be viewed by administrators. Those Administrators can only view certain information. SSN is now blanked out.

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain. No consolidation of processes.

8) How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

Data is viewed on an as needed basis by the FMS Help Desk and Data Access Control. Privacy Information is blocked out to these users. Information is retrieved based on Name.

9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

Only queries can done to search for a specific user by name, application, specific platform resource. Queries cannot be done on privacy information.

10) What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.)

Individuals can decline to provide Social Security Number, as it is optional. All other information is needed so we can mail information or contact the user. If the user declines, that user cannot have access to FMS systems.

D. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

System is part of Lotus Notes, and works the same as any other Lotus Notes Application.

2) **What are the retention periods of data in this system?**

Retention periods are designed in the Data Access Control Division's retention plan, as approved by AC Management. Retention of data is for 5 years after user access is withdrawn.

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

As stated earlier, no reports are generated from this system. Data will be purged after retention period has lapsed.

4) Is the system using technologies in ways that the FMS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)? No.

5) How does the use of this technology affect public/employee privacy? N/A.

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain. No.

7) What kinds of information are collected as a function of the monitoring of individuals? N/A.

8) What controls will be used to prevent unauthorized monitoring?
Access Controls are in place on the database to prevent unauthorized access.

9) Under which Privacy Act systems of records notice does the system operate?
Provide number and name.

.014 - Debt Collection Operations System

10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

System is not being modified.

E. ACCESS TO DATA:

1) Who will have access to the data in the system? (E.g., contractors, users, managers, system administrators, developers, other)

Access to the data, as stated above is to the FMS Help Desk, and Data Access Control Division Employees and Contractors. Specific Privacy information is blanked out for all users.

2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

Based on responsibility of the individuals, Help Desk and DACD personnel have access so that they can help the user, when that user calls in for assistance. The information in the database helps the Help Desk and DACD to ensure that the person they are talking to is indeed the person who has the accounts.

3) Will users have access to all data on the system or will the user's access be restricted? Explain.

Access is restricted for the Help Desk Personnel by viewing the individuals Profile information. This gives the users Name, Agency, Telephone Number and PIN.

4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list materials)processes and training

All FMS Contractors and Employees are required to go through yearly Security Training.

5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?

Yes, and they are under the same control as any contractor at FMS, which only allows access on a need to know basis, with proper Security Clearance upon FMS contractor employment.

6) Do other systems share data or have access to the data in the system? If yes, explain.

No.

7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

No Public individuals have data in this system. This is not an "interface", but a stand alone system used solely in tracking that requests for access to FMS systems. The

database is blanked out where SSN numbers use to be, and users can not view that information.

8) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)? No.

9) How will the data be used by the other agency? N/A.

10) Who is responsible for assuring proper use of the data? N/A.